Before the
Federal Communications Commission
Washington, D.C. 20554

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | WC Docket No. 16-106 (FCC 16-39) |
| Protecting the Privacy of Customers of | ) | |
| Broadband and Other Telecommunications | ) | |
| Services | ) | |

REPLY COMMENTS OF THE NATIONAL CONSUMERS LEAGUE

# Executive Summary

The National Consumers League ("NCL") reiterates its support for the Federal Communications Commission's ("FCC" or the "Commission") data security and data breach notification proposals. Because sensitive data cannot be separated from non-sensitive data without intrusive methods, NCL urges the Commission to consider all data that the broadband internet access service ("BIAS") providers collect as deserving of equal protections under the proposed Rules. Specifically, NCL urges the Commission to implement strong baseline data security and breach notification rules that will serve to provide robust protection for BIAS customers' data.

In our reply comments, NCL responds to various statements in the record made by interested parties in the Commission's broadband privacy Notice of Proposed Rulemaking ("NPRM"). We reiterate that the FCC has requisite authority to regulate BIAS providers. Furthermore, we argue that the existence and prominence of edge providers and data

brokers does not affect the Commission's mandate to protect consumer privacy of data shared by BIAS provider customers with the BIAS providers themselves. The proposed rules are justified given the unique role of ISPs in the internet ecosystem. Despite what some commenters claim, these data security and breach notification rules merely set high baseline protections for consumers that include common-sense security measures such as multi-factor authentication ("MFA"). BIAS providers are free and encouraged to innovate above these minimum standards. BIAS providers are also not disadvantaged against other parties in any way; the Commission's rules would only apply when related to communications-related services.

# Table of Contents

# Introduction

The National Consumers League respectfully submits the following comments in the above-captioned docket.[1]

NCL is America's pioneering consumer advocacy organization, representing consumers and workers on marketplace and workplace issues since our founding in 1899.[2] NCL also hosts and maintains Fraud.org, a website dedicated to giving consumers the information they need to avoid becoming victims of telemarketing and Internet fraud. NCL issues a bi-weekly publication, the #DataInsecurity Digest, which delivers important consumer-focused data security news, policy, and news analysis to consumers. NCL's comments focus primarily on the data security and data breach notification provisions of the NPRM.

# I. The FCC's Authority to Regulate BIAS Providers as Common Carriers Has Been Upheld by the Courts

[1] NCL gratefully acknowledges the invaluable assistance provided by Michael Benedetti (University of Dayton School of Law '17) and Taesung Lee (Georgetown Law '15) in preparing NCL's comments and reply comments in this proceeding.
[2] National Consumers League, *Mission*, http://www.nclnet.org/mission (last visited June 20, 2016).

The D.C. Circuit Court of Appeals recently upheld the Commission's 2015 Open Internet Order in *US Telecom v. FCC*.[3] This decision reaffirmed the Commission's reclassification of both fixed and wireless broadband providers as telecommunications services—subject to regulation as common carriers under Title II of the Communications Act. As a result of this decision, the FCC has clear statutory authority to regulate BIAS providers.

While the Federal Trade Commission ("FTC") is commonly viewed as the primary agency responsible for consumer protection in the privacy and data security areas, other federal agencies have such authority over particular industry sectors. For instance, the Office for Civil Rights in the Department of Health and Human Services is responsible for enforcing Health Insurance Portability & Accountability Act ("HIPAA"), the Consumer Financial Protection Bureau is responsible for enforcing the Gramm–Leach–Bliley Act ("GLBA"), the Department of Education is responsible for enforcing Family Educational Rights and Privacy Act ("FERPA"), and the FTC and FCC jointly enforce the Telephone Consumer Protection Act ("TCPA"). Furthermore, the FCC itself has a mandate to protect consumer privacy. As Georgetown Law Professor Paul Ohm succinctly put it, "[t]he law protects what it protects, and the burden should be on those who would rewrite the statute, not on the agency that implements it."[4] Thus, the FCC as the expert agency in

[3] *United States Telecom Association v. FCC*, No. 15-1063 (D.C. Cir.), https://www.cadc.uscourts.gov/internet/opinions.nsf/3F95E49183E6F8AF85257FD200505A3A/$file/15-1063-1619173.pdf.

[4] Paul Ohm, *Before the Subcommittee on Communications and Technology Committee on Energy and Commerce U.S. House of Representatives*, June 14, 2016, at 3, http://docs.house.gov/meetings/IF/IF16/20160614/105057/HHRG-114-IF16-Wstate-OhmP-20160614.pdf (*Ohm Comments*).

telecommunications has the relevant experience, motivation, and legal power to regulate to protect consumers who are facing growing threats in this area.

# II. Data Breaches are on the Rise

A Ponemon Institute study found that cybersecurity incidents continue to grow "in both volume and sophistication, with 64 percent more security incidents reported in 2015 than in 2014."[5] Further, the average cost of a data breach for the surveyed companies has increased 29 percent since 2013 to $4 million (approximately $158 per compromised record). There is a mixed trend with companies being held liable for the breaches, which emphasizes the importance of strong data security and breach notification standards so that consumers are properly protected.[6]

According to data collected for the National Telecommunications & Information Administration ("NTIA") in July 2015 by the U.S. Census Bureau, 19 percent of Internet-using households reported that they had been affected by an online security breach, identity theft, or similar malicious activity during the 12 months prior to the July 2015 survey.[7]

[5] *IBM & Ponemon Institute Study: Data Breach Costs Rising, Now $4 million per Incident*, IBM, June 15, 2016, https://www-03.ibm.com/press/us/en/pressrelease/49926.wss.
[6] *See* Nicole Hong, *For Consumers, Injury Is Hard to Prove in Data-Breach Cases*, The Wall Street Journal, Jun. 26, 2016, http://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988.
[7] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activity*, NTIA, May 13, 2016, https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

While it may be true that non-BIAS entities have suffered more breaches and enforcement actions than BIAS providers have suffered, the trend of BIAS providers purchasing and consolidating with so-called "big data" and advertising companies creates a greater attack surface due to the larger aggregation of data.[8] This risk is magnified when BIAS providers merge data collected via a BIAS telecommunications service with data that is collected as a result of non-communications related service.

# III. BIAS Providers have Unique Access to Customer Data

BIAS providers argue that they have neither unique nor comprehensive access to data on customers' internet activity. They cite repeatedly a working paper by Peter Swire[9] ("Swire Paper"), which states that ISP access to consumer data is limited and often less comprehensive than other players in the internet ecosystem due to the rise of HTTPS encryption, virtual private networks (VPNs), and the move to a mobile internet economy.[10] However, Georgetown Law Professor Ohm states that BIAS providers indeed have a privileged place as the bottleneck between the customer and the rest of the internet: this unique vantage point gives BIAS providers "the ability to see at least part of every single

[8] *See generally Big Data is Watching: Growing Digital Data Surveillance for Consumers by ISPs and Other Leading Video Providers*, Center for Digital Democracy, Mar 2016, https://www.democraticmedia.org/sites/default/files/field/public-files/2016/ispbigdatamarch2016.pdf (*Big Data CDD*).

[9] *See generally* Peter Swire, Justin Hemmings, & Alana Kirkland, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, The Institute for Information Security & Privacy at Georgia Tech, Feb. 29, 2016, http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf.

[10] *See* Comments of CTIA, *Protecting the Privacy of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, filed May 26, 2016, at 7 (*CTIA Comments*); *See also* Comments of Comcast, *Protecting the Privacy of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, filed May 27, 2016, at 5 (*Comcast Comments*).

packet sent to and received from the rest of the Internet."[11] Congress has long expressed its intent to broadly protect the metadata gathered through these types of bottlenecked communication channels. In the 1996 Telecommunications Act, Congress "decided to impose significant limits on what telephone companies could do with the list of numbers an individual customer calls . . . [t]he list of websites visited by an individual is even more private, individual and sensitive than those older lists of telephone contacts."[12] Professor Ohm correctly points out that this intent to protect metadata has only intensified as customers are switching to more data-rich internet services. BIAS providers also ignore the rebuttals made by Princeton Professor Nick Feamster[13] and Upturn.[14]

The claim that ISPs have only limited access to customer data is inaccurate. The Upturn report clarifies this misconception with four critical arguments.[15] First, the report notes that widespread encryption is still a long way off due to various technical considerations. While encryption adoption has grown, a substantial portion of internet activity remains unencrypted and freely accessible to ISPs. According to Upturn, 86 percent of health websites, 90 percent of news websites, and 86 percent of shopping websites are among these unencrypted figures.[16] These figures include popular websites such as Mayo Clinic, the New York Times, and Target. Such websites contain highly sensitive health

[11] *Ohm Comments* at 3; *See also Id.* ("No other entity on the Internet possesses the same ability to see. If you are a habitual user of the Google search engine, Google can watch you while you search, and it can follow you on the first step you take away from the search engine. After that, it loses sight of you, unless you happen to visit other websites or use apps or services that share information with Google").
[12] *Ohm Comments* at 4.
[13] Nick Feamster, Princeton University, March 3, 2016, https://ftt-uploads.s3.amazonaws.com/fcc-cpni-nprm.pdf.
[14] Aaron Rieke, David Robinson, Harlan Yu, *What ISPs Can See*, Upturn, Mar 2016, https://www.teamupturn.com/reports/2016/what-isps-can-see (*Upturn Report*).
[15] *Id*.
[16] *Id.* at 3-4.

information, political and social preferences, and detailed shopping behavior—all of which are currently accessible to BIAS providers.

Further discrediting the BIAS providers' claims on this point, Upturn points out that many of the figures referenced in the Swire Paper fail to discriminate between the different types of data that are encrypted on websites. While graphic-intensive video streaming websites such as Netflix, which itself accounts for roughly 35 percent of North American internet traffic, are moving towards encryption, websites such as WebMD, which generate far less traffic but contain much more personalized data, remain unencrypted.[17] The Upturn report also notes how the increasing number of so-called Internet of Things devices often relies on unencrypted transmissions. Second, even with encryption, ISPs are still able to see which domains are being visited. The report details a scenario in which seemingly unrelated bits of information may be collected through encrypted internet traffic and patched together to reveal highly sensitive information. The example given is an individual visiting abortionfacts.com, followed by plannedparenthood.com, followed by dcabortionfund.org, followed by maps.google.com. Clearly this method of data collection and retention can be used to paint vivid pictures of ISP customers. These pictures only expand in scope and in clarity over time. Third, the Upturn report illustrates how surprisingly revealing encrypted internet traffic can be. By analyzing aspects such as packet size, time, and destination (the metadata), ISPs are able to infer much of the online behavior of their customers with surprising accuracy.

[17] Sandvine, *Global Internet Phenomena Spotlight: Encrypted Internet Traffic*, 2015, at 4, https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf.

Finally, the Upturn report states that VPNs are not as popular as suggested, refuting a study cited in the Swire Paper indicating that 16 percent of North Americans have used VPNs.[18] The Upturn report correctly points out that this figure is comprised of any North American who has ever used a VPN, and not those that use one on a consistent basis. Furthermore, VPNs can be costly, slow, and are often technically challenging to set up properly. Even Opera's "free" new Opera VPN service will be monetized through the insertion of advertisements and the sale of anonymized collections of data acquired from users of Opera VPN.[19] It should also be noted that Opera's share of the browser market is very low. As of April 2016, Opera accounted for just 2 percent of the global user share as measured by U.S. analytics vendor Net Applications.[20]

BIAS providers also portray edge providers as having more comprehensive access to consumer data. While edge providers certainly do have a different perspective when viewing customer information, their window of access is no more inclusive. In fact, edge providers have even more limited access. Users of edge provider services have access to an abundance of free and open source anti-tracking tools, such as AdBlock, NoScript, or HTTPS Everywhere, that restrict monitoring and retention of data.[21] Regardless of the tool a consumer chooses to use to restrict access by edge providers to her data, all of her data,

[18] Jason Mander, *GWI Infographic: VPN Users*, GlobalWebIndex, October 24, 2014, http://www.globalwebindex.net/blog/vpn-infographic.
[19] Gregg Keizer, *Opera offers iPhone users free VPN, with strings attached*, Computerworld, May 10, 2016, http://www.computerworld.com/article/3068652/apple-ios/opera-offers-iphone-users-free-vpn-with-strings-attached.html.
[20] *Id.*
[21] Bill Snyder, *Firefox's new anti-tracking tool features best Chrome and Edge*, CIO (Oct 27, 2015), http://www.cio.com/article/2998181/consumer-electronics/firefoxs-new-anti-tracking-features-best-chrome-and-edge.html.

passes through the bottleneck of the ISP. In light of abundance of popular unencrypted services, and accounting for how revealing metadata can be, ISPs gain overwhelming access to customer information through their unique position in the internet ecosystem. While edge providers cannot exist without ISPs, ISPs can exist without edge providers.[22]

Another concern BIAS providers cite is that as customers hop between various ISP networks (i.e. home, office, mobile), their access to customer data becomes fractured and incomplete. While it is true customers can easily switch between ISP networks, and this behavior can sometimes splinter ISP access, there is still an abundance of data that passes through each of these channels.[23] Further, customers who hop between ISPs on a daily basis often connect to the same networks routinely, and over time each of these networks can collect significant amounts of data on mobile customers.[24] Thus, even if there may be gaps in access, this growing source of data deserves no less protection from BIAS providers.

# IV. The Proposed Rules Would Not Put BIAS Providers at an Unfair Disadvantage to Edge Providers

Some BIAS providers argue that the Commission's proposed Rules would put them at a competitive disadvantage against edge providers, particularly in advertising. However,

[22] *See also Upturn Report* (It is true that today, many consumers' personal Internet activities are spread out over several connections: a home provider, a workplace provider, and a mobile provider. However, a user often has repeated, ongoing, long-term interactions with both her mobile and her wireline provider. Over time, each ISP can see a substantial amount of that user's Internet traffic).
[23] *Upturn Report*.
[24] *Id*.

as Ohm argues, "[n]othing in the law or proposed rules prevents a broadband internet provider from entering into direct competition with search engines or other edge providers."[25] Although BIAS providers' use of certain types of data would be restricted under the proposed rules, those restrictions would only apply to data that is collected and used as part of the providers' communications services. Opponents of the Commission's proposed rules also seem to ignore the special relationship that customers have with their BIAS providers: customers pay BIAS providers in order to access internet services as opposed to giving up data about themselves in order to utilize "free" edge services.

The Communications Act does not require the FCC to support ISPs' efforts to compete in the advertising sector.[26] However, the Commission's proposed rules will apply to ISPs that collect and utilize data in pursuance of communications-related services and ensure a level playing field in this relevant industry. This competition argument is also misleading when ISPs themselves enjoy and assert incumbent power in a market with high barriers to entry.[27]

---

[25] *Ohm Comments* at 7; *See also Id.* "Likewise, if a search engine company decides to create a broadband Internet service (say a subsidiary that provides residential fiber optic service), it will fall within Title II of the Communications Act and thus be subject to the FCC's new rules. In either case, the two competing companies will be subjected to precisely the same rules under precisely the same terms. What BIAS providers truly mean when they complain about unfair or discriminatory treatment is that a particular privacy law to which they are subject—section 222 of the Communications Act—protects privacy too much."

[26] https://transition.fcc.gov/Reports/1934new.pdf

[27] Jon Brodkin, *One big reason we lack Internet competition: Starting an ISP is really hard*, Ars Technica, April 6, 2014, http://arstechnica.com/business/2014/04/one-big-reason-we-lack-internet-competition-starting-an-isp-is-really-hard/ ("Financial analysts last year estimated that Google had to spend $84 million to build a fiber network that passed 149,000 homes in Kansas City...A national Google Fiber build out passing 15 percent of US homes would cost $11 billion a year for five years, Wall Street analysts have estimated"); *See also* Jon Brodkin, *AT&T gave $62K to lawmakers months before vote to limit muni broadband*, Ars Technica, Feb 26, 2016, http://arstechnica.com/tech-policy/2016/02/att-gave-62k-to-lawmakers-months-before-vote-to-limit-muni-broadband/ ("AT&T's opposition to municipal broadband is well-known").

# V. The Proposed Rules Will Not Hamper Innovation or Impose Unnecessary Costs on BIAS Providers

Despite claims that the Commission's reclassification of BIAS as a common carrier under Title II will discourage investment and impose costs, the telecommunications industry had a strong financial year in 2015.[28] For instance, AT&T's net income was over $13 billion, which marked a 60 percent increase from 2014.[29] Despite these profits, the FCC, in its 2016 Broadband Progress Report, found that "[a]pproximately 51 percent of Americans have one option for a provider of 25 Mbps/3 Mbps fixed broadband service … and approximately 10 percent of Americans have no options for 25 Mbps/3 Mbps fixed broadband service."[30] Despite these increased profits and a lack of competition, BIAS providers continue to argue that the Commission's broadband privacy rules will only discourage innovation and investment.

Furthermore, ISPs continue to "innovate" in the areas of data collection. Many ISPs have incorporated more data collection and digital marketing technologies in order to collect and analyze huge amounts of consumer data. In a recent paper, the Center for Digital Democracy points to the enormous amount of data that ISPs already collect, and note the numerous acquisitions and partnerships that enable ISPs to collect more and target

[28] Kate Cox, *Did Net Neutrality Kill Broadband Investment Like Comcast, AT&T, Verizon Said It Would?*, Consumerist, February 9, 2016, https://consumerist.com/2016/02/09/did-net-neutrality-kill-broadband-investment-like-comcast-att-verizon-said-it-would/.
[29] AT&T Inc., *2015 Annual Report*, February 18, 2016, at 11, https://www.att.com/Investor/ATT_Annual/2015/downloads/att_ar2015_completeannualreport.pdf.
[30] FCC, *2016 Broadband Progress Report*, January 29, 2016, at 38, https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-6A1.pdf.

"better" based on the data.[31] This desire to expand data-gathering and advertising technology is the reason that Verizon purchased AOL for $4.4 billion in 2015, and why Verizon and AT&T are reportedly each bidding in excess of $3 billion for Yahoo today.[32]

ISPs argue that these regulatory burdens are not reflective of customers' demands. However, a 2015 NTIA survey found that 84 percent of respondents admitted that they had at least one concern about online privacy and security risks while 40 percent cited at least two different concerns.[33] A 2015 Pew Report found that many Americans were not confident that companies that collect data about them could keep that information private and secure.[34]

# VI. Limitations of the Current FTC Framework

Opponents of the Commission's proposed rules argue for a flexible approach that would be heavily informed and enforced by industry. These opponents reject a need for common-sense, FCC-mandated risk assessments, penetration testing, and technical audits.[35] It should be noted that the FCC has not set down the specifics of how these

---

[31] *Big Data CDD* at 4, 8, (For example, Verizon acquired both AOL and Millennial Media in 2015. Comcast bought ad-technology companies Visible World, which included AudienceXpress, in 2015 and FreeWheel Media the previous year. Through its acquisition of DirecTV, AT&T gained a major new way to use data to target its customers.).

[32] Mike Shields & Thomas Gryta, *Verizion Agrees to Buy AOL for $4.4 Billion*, Wall Street Journal, May 12, 2015, http://www.wsj.com/articles/verizon-to-buy-aol-for-4-4-billion-1431428458; Greg Roumeliotis, *Exclusive: Verizon, AT&T set to make final round of bids for Yahoo web assets - sources*, Reuters, June 13, 2016, http://www.reuters.com/article/us-yahoo-m-a-verizon-exclusive-idUSKCN0YZ0C8.

[33] *Id.*

[34] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Research Center, May 20, 2015, http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

[35] *See CTIA Comments* at 165.

security assessments must be conducted, merely that BIAS providers are under legal obligation to conduct them. Without minimum baselines, the BIAS providers are accountable only to themselves because there would be no enforceable legal standards. While the FTC conducts workshops and promulgates best practices, these are merely recommendations and do not address the FTC's main limitation: that its case-by-case enforcement actions are reactive, rather than proactive.

The FTC, in its enforcement actions, has required companies to have a "written comprehensive information security program that includes a designated official to run the program, an annual risk assessment, appropriate safeguards to address risks, service provider supervision, and periodic re-assessment of the program."[36] The FTC, in its comment in this proceeding, stated "this approach protects consumers from lax data security practices, while also giving businesses the flexibility to tailor their programs to their particular circumstances."[37] Some BIAS providers argue that the FCC should adopt the FTC-style approach, yet argue that the FCC should not mandate common things that are required in the consent decrees. BIAS providers cannot have it both ways. Furthermore, there have been continual efforts to gut the FTC's ability to protect consumers, despite the FTC's current lack of APA rulemaking authority.[38]

[36] FTC, *Start with Security: A Guide for Business*, June 2015, https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business; Comments of FTC, *Protecting the Privacy of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, filed May 27, 2016, at 27 (*FTC Comments*).
[37] *Id*.
[38] *Pallone Assails Republican Efforts to Gut the FTC*, Committee on Energy & Commerce Democrats, June 9, 2016, https://democrats-energycommerce.house.gov/newsroom/press-releases/pallone-assails-republican-efforts-to-gut-the-ftc.

Opponents to the Commission's rules also argue that BIAS providers have an incentive to not exploit or fail to meet customer expectations because they would not otherwise be able to attract and retain customers.[39] This ignores the fact that ISPs continue to prosper despite the fact that they consistently rank in the bottom of customer experience surveys due to a lack of competition.[40]

# VII. Multi-Stakeholder Approach Should Not Be Used to Establish Enforceable Data Security Standards

The multistakeholder approach should not be the primary avenue for establishing minimum data security baselines. As NCL stated in prior comments, the multistakeholder approach has notably failed to produce effective voluntary standards in related areas such as mobile app transparency and facial recognition.[41] As Georgetown Law Professor and former FTC Commissioner David Vladeck states, "you don't simply allow industry to decide what to do in a way in which they don't have any incentive to compromise."[42] NCL argues that any use of the multistakeholder process should not supplant the rules but instead serve as a guideline for implementation. Furthermore, NCL reiterates our suggestion that an appropriate FCC advisory committee, such as the Technological Advisory Council,

---

[39] Comments of CenturyLink, *Protecting the Privacy of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, filed May 27, 2016, at 2 (*CenturyLink Comments*).
[40] Jon Brodkin, *ISPs and pay-TV lowest-rated industries, with Comcast worst in sector*, Ars Technica, May 26, 2016, http://arstechnica.com/business/2016/05/isps-and-pay-tv-lowest-rated-industries-with-comcast-worst-in-sector/.
[41] Comments of NCL, *Protecting the Privacy of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, filed May 27, 2016, at 10 (*NCL Comments*).
[42] Natasha Singer, *Why a Push for Online Privacy Is Bogged Down in Washington*, The New York Times, Feb 28, 2016, http://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html?_r=0.

conduct regular meetings to discuss and update specific mandates to ensure that consumers are adequately protected against evolving threats.

# VIII. The FCC Should Adopt a Strong Baseline Data Security Standard

NCL believes that, in the BIAS context, sensitive and non-sensitive information should not be treated differently.[43] We are concerned that allowing BIAS providers to treat sensitive and nonsensitive information differently would "greatly increase compliance complexity and costs," all customer information in the BIAS context should be protected.[44] This treatment also makes sense due to the lack of a non-privacy invasive method in separating sensitive and nonsensitive information in the BIAS space.

BIAS providers argue that they already have robust data security measures in place to ensure that the customer data they gather is protected. However, there are numerous examples of these providers being targeted and successfully breached. For instance, in 2014, employees of AT&T improperly accessed customer records supposedly protected by these data security measures.[45] Once accessed, the employees distributed these records—which consisted of sensitive personal information—to third parties with the intent to illegally unlock mobile devices. AT&T became suspicious of these events as early as 2012, but failed to notify their customers or law enforcement until two years later. Due to this

[43] *See CTIA Comments* at 150.
[44] *Ohm Comments* at 6.
[45] *In the Matter of AT&T Services, Inc.*, DA 15-399, Order (rel. Apr. 8, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DA-15-399A1_Rcd.pdf.

negligence, over 50,000 customer records containing sensitive personal data were distributed without authorization.

In 2012, major Australian ISP AAPT fell victim to another security breach.[46] Confirmed by CEO David Yulie, members of the group Anonymous breached AAPT data security safeguards and successfully stole 40 gigabytes of business customer data. Members of Anonymous involved with the attack claimed that it was carried out in response to a governmental proposed data-retention scheme. These Anonymous members argued that an ISP incapable of keeping its own data secure would be incapable of securing even larger amounts of data collected through the government's proposed retention program.

Dell's SecureWorks security division recently uncovered another attack on more than a dozen ISPs resulting in the redirection of entire chunks of internet traffic for the purpose of stealing bitcoins and other cryptocurrencies.[47] This attack was carried out by hijacking a Canadian ISP staff account and using that account to broadcast false signals to redirect internet traffic. Other ISPs abroad have even been found purposefully deploying distributed denial of service ("DDoS") attacks in order to disrupt competing services and gain a competitive edge.[48] Thus there is ample evidence in the record to suggest that ISPs' existing data security protections may be insufficient to adequately protect the growing

[46] Michael Lee, *AAPT Confirms Data Breach as Anonymous Claims Attack*, ZD Net, July 26, 2012, http://www.zdnet.com/article/aapt-confirms-data-breach-as-anonymous-claims-attack/.
[47] Andy Greenberg, *Hackers Redirect Traffic From 19 Internet Providers to Steal Bitcoins*, Wired, Aug 7, 2014, https://www.wired.com/2014/08/isp-bitcoin-theft/.
[48] Jonathan A. Ophardt, *Cyber Warfare and the Crime of Aggression: the Need for Individual Accountability on Tomorrow's Battlefield*, Duke Law & Technology Review, 2010, http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1198&context=dltr.

attack surface that ISPs are creating by virtue of their large subscriber base and acquisition of advertising and other data-rich entities. To counteract this growing threat, BIAS providers should be required to follow the minimum, baseline standards suggested in the Commission's proposal. There is nothing in the proposal preventing BIAS providers from using their unique market insights to exceed these minimum data security standards, but they should undoubtedly be prohibited from falling beneath them.

Despite this evidence, many BIAS providers argue that the FCC should not impose prescriptive rules and minimum data security requirements. Some opponents of the rules argue that prescriptive regulations would encourage a compliance mindset, rewarding companies that meet minimum standards and discourag[e] innovation."[49] This is the exact opposite of what the rules would accomplish because ISPs would be free to innovate above the minimum baselines set out in the Commission's rules.[50]

For example, in the payment card industry, Verizon has helped to innovate beyond Payment Card Industry Data Security Standard (PCI DSS) by partnering with banks and using location data gathered from cellphones to score the risk of financial transactions.[51] If the transaction requires a cardholder to be present, and the location data determines that the cardholder is actually 500 miles away, the data indicates a higher likelihood of fraud. NCL reiterates that the Commission's baselines will not "[m]ake it easier for

[49] *CTIA Comments* at 151.
[50] §54.7005(a) data security rules have certain "[a]t a minimum" requirements.
[51] *Verizon 2015 PCI Compliance Report*, at 7, http://www.verizonenterprise.com/placeholder/resources/reports/rp_pci-report-2015_en_xg.pdf

cybercriminals."[52] It is not a credible argument to say that ISPs should not implement MFA because bad actors would now know that MFA protection exists: the benefit of MFA is that there is additional protection when some information is stolen (i.e. password) and not others (i.e. access to one's email account for password reset verification). MFA does impose additional costs, but also provides robust protection of customer data. Further, MFA is something increasingly done by edge providers (i.e. Google and Facebook) that ISPs are trying to emulate.[53]

Moreover, mandatory employee training is a common-sense best practice. Security is an issue that affects the company as a whole, especially when employee error is the main cause of data breaches today.[54] Despite these risks, a 2016 Ponemon Institute study found that awareness of this risk is not influencing companies to put practices in place that will improve the security culture and training of employees. Only 35 percent of surveyed companies said that senior executives believe it is a priority that employees are knowledgeable about how data security risks affect their organizations. 60 percent of respondents believe employees are not knowledgeable or have no knowledge of the company's security risks.[55]

---

[52] *CTIA Comments* at 151.
[53] *See CTIA Comments* at 171-2.
[54] *2016 Data Breach Investigations Report,* Verizon, at 40 *available at* http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016 (*Verizon Breach Report*); *NCL Comments*; Ponemon Institute LLC, *Managing Insider Risk through Training & Culture*, Sponsored by Experian Data Breach Resolution, May 2016, https://www.experian.com/assets/data-breach/white-papers/experian-2016-ponemon-insider-risk-report.pdf.
[55] *Id*.

Some claim that the FCC mandated data security rules such as performing annual assessments and designating a senior official responsible for the BIAS provider's information security program, would be too costly for BIAS providers. However, NCL takes the position that protecting consumers' data is a part of running a modern company.[56] More than 90 percent of breaches began with a phishing attack, something that can be mitigated with good employee training and an information security officer.[57]

Similarly, it is incorrect to assert that mandating a minimum baseline for authentication in protecting consumer data would be too costly for small to medium sized carriers. To address this concern, NCL suggests that the FCC to allow third party authentication such as OAUTH and OpenID as an alternative to developing and implementing a first party solution for these carriers.

Finally, §64.7005(a) requires that a "BIAS provider must ensure the security, confidentiality, and integrity of all customer PI the BIAS provider receives, maintains, uses, discloses, or permits access to from any unauthorized uses or disclosures, or uses exceeding authorization" (emphasis added). Opponents to the FCC's rules argue that a strict liability standard without a safe harbor or intent element would unfairly penalize

[56] Comments of ACA, *Protecting the Privacy of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, filed May 27, 2016, at 23, 25 (*ACA Comments*).
[57] Nicole Perlroth, *A Computer Security Start-Up Turns the Tables on Hackers*, The New York Times, June 12, 2016, http://www.nytimes.com/2016/06/13/technology/a-computer-security-start-up-turns-the-tables-on-hackers.html.

BIAS providers. FTC supports the development of data security safe harbors, but "only if they include strong and concrete requirements backed by vigorous enforcement."[58]

# IX. A 10-Day Breach Notification Standard Is Not Overly Burdensome

Many BIAS providers argue that the proposed 10-day breach notification requirement included in the NPRM is unreasonable and should not be adopted by the FCC.[59] AT&T calls the requirement "draconian."[60] Comcast says the 10-day requirement "is the lowest amount of time [they] have ever seen in a data breach law."[61] Supporting this stance, BIAS providers cite among other things the many state laws in the area of breach notification. These laws primarily range between a 30 and 90-day requirement to notify affected customers.[62]

While these state breach notification laws are worthy of consideration, NCL believes the FCC's proposed 10-day notification requirement is more appropriate. Notifying users and regulators of cyber incidents and data leaks is important because it makes transparent the frequency of cybercrimes and helps companies share information about breaches.

---

[58] *FTC Comments* at 29, ((1) a requirement that participants implement substantially similar or more robust requirements than those contained in the Rule; (2) an effective, mandatory mechanism for the independent assessment of participants' compliance with the requirements; and (3) disciplinary actions for noncompliance).
[59] *Comcast Comments* at 63; Comments of AT&T, *Protecting the Privacy of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, filed May 27, 2016, at 82 (*AT&T Comments*).
[60] *AT&T Comments* at 82.
[61] *Comcast Comments* at 63.
[62] Perkins Coie LLP, *Security Breach Notification Chart* (rev. Jan. 2016), https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.

Moreover, it helps to keep companies accountable, deterring behavior such as AT&T's, where they delayed informing their customers that they were breach victims for years.[63]

When data is stolen, its usefulness to hackers immediately begins to devalue.[64] This is due to the fact that once data is stolen, affected parties are more likely to discover the breach as time goes on. Once the breach is disclosed publicly, affected parties can take necessary steps to combat the breach and protect themselves from harmful consequences such as fraud or identity theft. Thus, stolen data is perishable and the market for it decreases over its lifetime. The 10-day notification law proposed by FCC would significantly hinder this market for stolen data. If BIAS providers were required to notify affected customers in a truly expedited manner and offer those customers steps to take to combat the breach, consumers could act more quickly to protect their information. Quick notification matters: a 2014 Ponemon Institute study found that 68 percent of consumers surveyed took some steps to protect themselves after being notified of a data breach.[65]

Also, this 10-day notification requirement is in a sense future-proofing breach notification for years to come. Many experts and state attorney generals are pointing to current breach notification standards and calling existing deadlines between 30 and 90 days far too long under many circumstances.[66] California Attorney General Kamala Harris

---

[63] *In the Matter of AT&T Services, Inc*. at 2813.

[64] Anna Nagurney, *A Multiproduct Network Economic Model of Cybercrime in Financial Services*, University of Massachusetts, September 2014 (Revised Jan 2015), https://supernet.isenberg.umass.edu/articles/MultiProduct_Network_Economics_of_CyberCrime.pdf.

[65] Ponemon Institute LLC, *The Aftermath of a Data Breach: Consumer Sentiment*, Sponsored by Experian Data Breach Resolution, April 2014, at 5, http://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf.

[66] Kamala D. Harris, *California Data Breach Report*, California Department of Justice, Feb 2016, https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

believes that "what constitutes a reasonable time for notification today might be unreasonable tomorrow, as technological improvements allow for faster forensic analysis, cheaper and more effectively targeted notice, and an improved ability by companies to quickly provide consumers with remedies."[67] As technology continues to evolve at an accelerating pace, this shorter, federal requirement seems far more appropriate for a forward thinking breach notification standard.

Other arguments BIAS providers present are that this expedited notification requirement could lead to over notification, notice fatigue, and general customer confusion.[68] Verizon argues that "customers will receive notifications that they do not care about and that create unnecessary confusion and anxiety, such that customers could stop paying attention to notices altogether and miss those that might actually be important."[69] In its previously submitted comments, NCL cited evidence that dispelled the myth of customer notice fatigue.[70] Furthermore, NCL believes that the value generated through prompt notification significantly outweighs the potential risks. A recent Ponemon Institute study found that the average time to identify a breach was estimated at 201 days, and the average time to contain a breach was estimated at 70 days.[71] Consumers are deeply concerned with the security of their data and believe it is important to receive notice in the

[67] *Id*. at 5.
[68] *CTIA Comments* at 100; *Comcast Comments* at 44.
[69] Comments of Verizon, *Protecting the Privacy of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, filed May 27, 2016, at 69 (*Verizon Comments*).
[70] *NCL Comments*.
[71] *IBM & Ponemon Institute Study: Data Breach Costs Rising, Now $4 million per Incident,* https://www-03.ibm.com/press/us/en/pressrelease/49926.wss.

instance of a breach.[72] In fact, consumers are actually demanding even greater communication and remedies from business after breaches occur.[73]

BIAS providers bolster this warning of over-notification by imagining scenarios where customers would have to be informed in cases of negligible unauthorized access. For instance, Verizon offered a hypothetical where a customer service representative mistakenly enters an incorrect account number and thereby accesses a wrong account, triggering a breach violation and a requirement to send out notice to customers.[74] In cases such as this, NCL believes it would be permissible to offer a good faith exemption to the otherwise strict liability notification requirements.[75] Such an exemption should be narrowly tailored, and the BIAS provider should still be required to inform the FCC so this exemption is not abused, as cases like these could be symptoms of an underlying security problem at the BIAS provider.

Should the FCC contemplate a good faith exemption from consumer notification, NCL reiterates that law enforcement and the Commission should always be notified of breaches in the BIAS space, even inadvertent breaches. Despite claims that these notifications would divert resources, both on the part of BIAS providers and on the part of the government, these notifications would not impose burdensome costs—since BIAS providers already should be keeping track of security breaches—and notifications to law

[72] Ponemon Institute LLC, *2012 Consumer Study on Data Breach Notification*, Sponsored by Experian Data Breach Resolution, June 2012, at 2.
[73] Experian, *2015 Second Annual Data Breach Industry Forecast*, 2015, https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf.
[74] *Verizon Comments* at 68-9.
[75] *AT&T Comments* at 79.

enforcement would help establish data regarding the efficacy of the Commission's rules and assist in framing the existing cybersecurity landscape.

# X. Third Party Accountability Should Be Part of the Proposed Data Security Rules

BIAS providers should be required to take responsibility for information that they share with third parties. This is not only a reflection of the BIAS provider-customer relationship, but also a reflection of the FTC's privacy-by-design approach as BIAS providers continue to contract with third parties. Because the Commission's rules will apply equally to all BIAS providers, they will not be at a disadvantage when negotiating contracts with third parties.[76]

Similar to what NCL proposed in its comments, the FTC suggests requiring BIAS providers to contractually obligate their agents to give the BIAS providers notice of breaches.[77] The BIAS providers would then be required to provide breach notification to the affected consumers. This model ensures that the consumer would be receiving a breach notice from an entity with which the consumer has a pre-existing relationship, rather than from a potentially unknown agent.

# Conclusion

[76] *CTIA Comments* at 151.
[77] *FTC Comments* at 32.

Data breaches are something that can and do impact millions of consumers every year. BIAS providers argue that the current framework is working to protect against such scenarios and so the new rules of the FCC's proposal are unwarranted. However, given the increasing frequency and cost of data breaches and BIAS providers' unique position in the internet ecosystem, there should be legally enforceable standards that will require them to properly secure their customers' information.

NCL believes that the robust data security measures outlined in the Commission's proposal are an important and appropriate way to better protect consumers' sensitive data. By encouraging BIAS providers to meet minimum baseline standards, data security will be significantly strengthened. By encouraging a prompt breach notification standard, consumers and law enforcement alike will be empowered to take proactive steps to combat the harmful effects that often follow a breach. NCL recognizes that the implementation of these rules might add additional costs to BIAS providers' operations. However, these costs are not overly burdensome, given the growing costs to consumers and businesses of breaches.

The proposed rules do not unfairly discriminate against BIAS providers, and they do not place them at an unfair disadvantage against competitors in spaces outside the common carrier's' primary business. Instead these rules allow the FCC, as the expert agency, to fulfill its mandate to protect consumers' data in the context of BIAS.

Respectfully submitted,